Kentucky Health Benefit Exchange

Privacy and Security Handbook

Updated: July 22, 2020

Table of Contents

Purpose

This document serves as a reference document to the Privacy and Security Training. Reviewing this document does not count towards completing the Privacy and Security Training course on My Purpose.

1. Introduction

It is of the utmost importance and a legal requirement to always be aware of the privacy and security of handling individuals' personal information. While performing kynector duties, you are exposed to sensitive client information, or **Personally Identifiable Information** (PII). PII includes the following:

- Full Name
- Date and place of birth
- Telephone number
- Address
- Mother's maiden name
- Social Security Number
- Medical, educational, financial, and/or employment information
- Driver's license number
- Email address
- Biometric records or identifiers

kynectors **must** handle PII carefully.

- Do not leave PII out in public areas where others may be able to access the information.
- Always discard PII in a shredder, not a trash can or recycling bin.
- Do not take pictures of PII using a personal cellphone or other personal devices.

There are serious legal and personal consequences for breaching privacy and security laws. It is important you understand the Federal guidelines in addition to internal office policies of the Kentucky Health Benefit Exchange.

2. HIPAA

Established in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is a federal law that primarily aims to:

1. Make it easier for people to keep health insurance.
2. Protect the confidentiality and security of healthcare information.
3. Help the healthcare industry control administrative costs.

HIPAA is comprised of various rules and regulations, which apply to covered entities and their business associates. Individuals, organizations, and agencies that meet the definition of a covered entity must comply with HIPAA's requirements to protect individually identifiable health information and provide patients with certain rights pertaining to that information.

If a covered entity works with a business associate, the entity must have a contract or other agreement with the business associate that establishes specifically what the business associate will do and requires the business associate to comply with the rules' requirements to protect the privacy and security of protected health information.

Please Note: *If covered entities and their business associates* ***do not*** *follow the HIPAA rules and regulations, they are directly liable and face severe penalties for the release of that information.*

Covered Entities

A **covered entity** is an organization that routinely handles protected health information. Below are some examples of covered entities:

Healthcare Provider

- Doctors
- Clinics
- Psychologists
- Dentists
- Chiropractors
- Nursing Homes
- Pharmacies

Please note that healthcare providers must transmit information in an electronic form in connection with a transaction that falls under the HIPAA standards. Also, government programs that pay for healthcare include Medicare, Medicaid, and the military and veterans' healthcare programs.

Health Plan

- Health insurance companies
- HMOs
- Company health plans
- Government programs that pay for healthcare

Information Exchange and Connection to other Patients

This includes entities that process nonstandard health information that they receive from another entity into a standard electronic format or data content, or vice versa.

Rules and Regulations

There are several rules and regulations that must be followed to maintain HIPAA compliance.

Rules	Description
Privacy Rule	• Establishes national standards to protect individuals' medical records and other personal health information.

Rules	Description
Security Rule	• Establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. • Requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
Enforcement Rule	• Contains provisions relating to compliance and investigations, the imposition of civil money penalties for violation of the HIPAA Administrative Simplification Rules, and procedures for hearings.
Breach Notification Rule	• Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. • Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers.
Transactions and Code Sets Standards	• Creates a uniform way to perform electronic data interchange (EDI) transactions for submitting, processing, and paying claims.
Employer Identifier Standard	• Requires employers have standard national numbers that identify them on standard transactions. The Employer Identification Number (EIN) is the identifier for employers and is issued by the Internal Revenue Service (IRS).
National Provider Identifier (NPI) Standard	• The NPI is a unique identification, 10-digit number for covered healthcare providers. Covered healthcare providers and all health plans and healthcare clearinghouses must use NPIs in the administrative and financial transactions adopted under HIPAA.

3. Protected Health Insurance (PHI) and Personally Identifiable Information (PII)

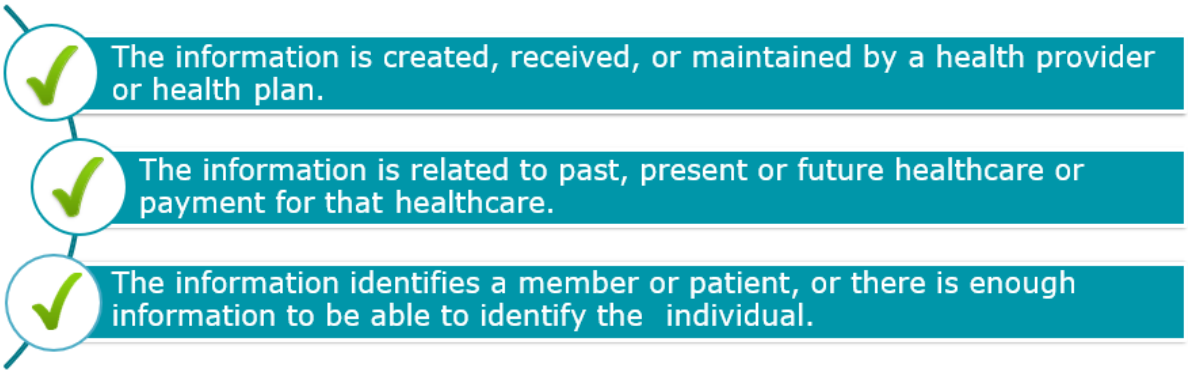
PII is defined as information which can be used to distinguish or trace an individual's identity when it's accessed alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual. Just as a reminder, common forms of PII are as follows:

- Full Name
- Date and place of birth
- Telephone number
- Address
- Mother's maiden name
- Social Security Number
- Medical, educational, financial, and/or employment information
- Driver's license number
- Email address
- Biometric records or identifiers

Protected Health Information (PHI)

The HIPAA Privacy Rule's purpose is to protect Individually Identifiable Health Information (IIHI). This information is also known as Protected Health Information (PHI) and is a subset of Personally Identifiable Information (PII).

For information to be considered PHI, it must meet all of the following conditions:



PHI Identifiers

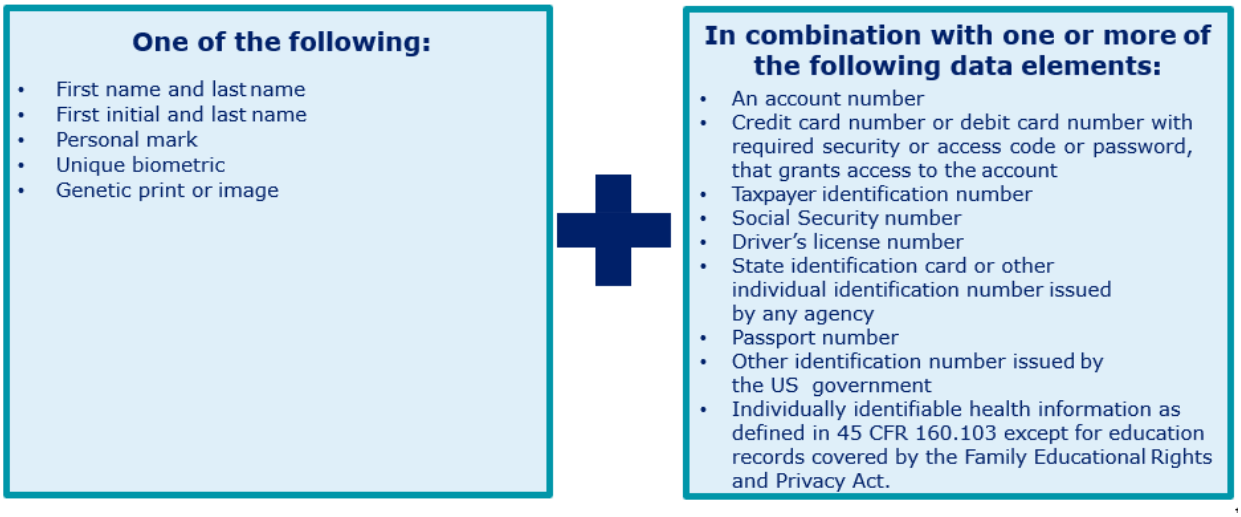
Public Health Information (PHI) is a subset of PII. PHI is defined as individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium. PHI includes the following 18 identifiers:

Data Element	Description
Name	First name, last name, maiden name combinations. It could be possible to identify an individual using a combination of data. (e.g. first name, zip code, street address etc.)
Geographic locators	Street address, city, precinct, zip code, latitude and longitude coordinates, etc.

Data Element	Description
Dates	Significant events in an individual's life - birth, death, marriage, admission, discharge, etc. The year is generally considered fine for use except in the case of the very elderly (>89 years of age; in which case they would be represented by an aggregate category (e.g. =>90).
Phone numbers	Personal, work, other mobile or land line numbers linked to an individual.
Fax numbers	Same as above.
Electronic mail addresses (email)	Same as above.
Social Security Number	9-digit number that continuously links an individual to his/her Social Security.
Medical record numbers	Medical record numbers can be used to identify individuals, if the individual also knew the institution that assigned it.
Health plan beneficiary numbers	Insurance card/member ID
Certificate/license numbers	Driver's license, birth certificate, etc.
Account numbers	Bank numbers, etc.
Vehicle identifiers and serial numbers, including license plate	Any vehicle characteristic that can help track down an individual.
Device identifiers and serial numbers	Medical devices with unique serial numbers, personal electronics, etc.
Web Universal Resource Locators (URLs)	Technology can now track individuals' locations and identities based on browser history and web site visits.
Internet Protocol (IP) address numbers	Similar to above.
Biometric identifiers, including finger and voice prints	Retinal images also fall into this category.

Data Element	Description
Full face photographic images and any comparable images	Visual aids that identify who you are.
Any other unique identifying number, characteristic, or code	This category is a "catch-all" that corresponds to any unique features that are not explicitly enumerated above.

KRS 61.931, further classifies Personal Information as:



The internal office policies and procedures of Kentucky are based on the overarching guidelines set forth by the Federal government. It is of the utmost importance and a legal requirement to always be aware of the privacy and security of handling individual's personal information.

While performing kynector duties, there is a high likelihood of being exposed to sensitive client information, or Personally Identifiable Information (PII). kynectors must handle PII carefully and should not leave it in public places or areas where others may be able to access to it.

kynectors **must follow** the below requirements at all times when working with PII:

- Papers or copies containing PII must never be left unsecure or in public places.
- When discarding PII, kynectors must use a shredder, not a trash can or recycling bin.
- kynectors must use a password protected computer.
- kynectors must lock their computer when they are away from the screen.
- kynectors never repeat PII aloud if others are nearby or could hear you over a phone call.

- PII is never be shared unless there is a business need.

It is critical for a kynector to follow the handling requirements to protect PII.

4. Security Breaches

A **security breach** is the unauthorized acquisition, distribution, disclosure, destruction, manipulation, or release of unencrypted or unredacted records or data that has resulted in or is likely to result in the misuse of personal information.

If the agency has a reason to believe that records or data subject to the unauthorized access may compromise the security, confidentiality, or integrity of the personal information and has resulted in or is likely to result in the misuse of the personal information or likelihood to harm one or more individuals, then the occurrence is considered a security breach.

Third party business partners of the Kentucky Health Benefit Exchange (KHBE) are responsible for ensuring the security of emails sent to KHBE containing confidential or personal information. There are certain precautions kynectors must take to limit the possibilities of a security breach.

KHBE business partners must use **secure email** if sending confidential information to KHBE staff.

Sending both a case number and name via email is a violation of PII. Please only send the **individual number or case number**.

Clean your desk of confidential data files and papers at the end of the day.

5. Kentucky Online Gateway

Kentucky Online Gateway (KOG) is an authentication services system for users requesting access to a variety of systems across the Commonwealth. kynectors must set up their personal account in KOG in order to access Resource Engine.

How do I create an Account?

1. Navigate to https://KOG.chfs.ky.gov/home and select that you are a **Citizen or Business Partner** and the select **Create Account**.
2. Enter all of your basic information and a valid email address on the registration screen, answer two security questions, and select **Sign Up**.
3. Navigate to the email inbox corresponding to the email address entered on the registration screen and find a **KOG Account Verification** message in your email inbox.
4. Open the **KOG Account Verification** email and click on the **activation link** to continue to the account creation process.
5. Register your mobile number (optional), click **Continue to Sign on**, and then sign into your KOG account to finish the account creation process and gain access to a variety of system interfaces and resources across the Commonwealth

Tips and Tricks for Navigating KOG

1. Use Google Chrome as your browser.
2. Use the Incognito browser within Google Chrome, if the computer is shared by multiple KOG users.
3. Clear the cache before logging into KOG or beginning registration.
4. Clear the cookies before logging into KOG or beginning registration

6. Penalties and Violations

See below for the consequences of violating privacy rules and procedures.

Civil Penalties
A violation that the covered entity was unaware of and could not have realistically avoided with a reasonable amount of care will result in a minimum fine of $100 per violation, up to a maximum of $25,000 per year.
A violation that the covered entity should have been aware of by exercising reasonable diligence will provoke a $1,000 fine for each violation, not exceeding $100,000 per year.
A violation suffered as a direct result of "willful neglect", in cases where an attempt has not been made to correct the violation will result in a minimum fine of $10,000, up to an annual maximum of $250,000
Violations due to willful neglect, not corrected, will result in a minimum fine of $50,000 per violation, up to a $1.5 million fine per year.

Criminal Penalties
Wrongful disclosure of Individually Identifiable Health Information (IIHI) can incur a maximum fine of $50,000 with up to 1 year of imprisonment.
Wrongful disclosure of Individually Identifiable Health Information (IIHI) committed under false pretenses could be up to a $100,000 fine with up to 5 years of imprisonment.
Wrongful disclosure of Individually Identifiable Health Information (IIHI) committed under false pretenses with the intent to sell, transfer, or use it for commercial advantage, personal gain, or malicious harm could be up to a $250,000 fine with up to 10 years of imprisonment.